

Amendments to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (CURRENTLY AMENDED) A keyless authorized access control system, the system comprising:

at least two object modules, each object module being assigned to a respective object; and

at least one identification device, each identification device having a microprocessor and a memory element;

wherein each identification device and the object modules have respective bidirectional data communications links between them for communicating encoded data, the data communicated between an identification device and ~~an~~ each object module being encoded using by an encryption algorithm that performs and a symmetric encryption method which uses an encryption parameter, wherein encryption algorithms and encryption parameters are respectively uniquely assigned to the object modules module;

wherein the memory element of each identification device stores at least two different encryption algorithms and at least two different encryption parameters including the encryption algorithms and the encryption parameters assigned to the object modules, wherein the microprocessor of an identification device selects one of from the stored encryption algorithms and encryption parameters the encryption algorithm and the encryption parameter assigned to an object module to be used with the symmetric encryption method for encoding the data to be communicated between the identification device and [[an]] the object module.

2. (ORIGINAL) The system of claim 1 wherein:

the encryption algorithm to be used for encoding the data to be communicated between the identification device and an object module is assigned by the identification device to the object module during a single initialization process between the identification device and the object module.

3. (CURRENTLY AMENDED) A keyless authorized access control system, the system comprising:

at least two object modules, each object module being assigned to a respective object, one of the object modules having a microprocessor and a memory element; and

at least one identification device, wherein each identification device and the object modules have respective bidirectional data communications links between them for communicating encoded data, the data communicated between an identification device and [[an]] each object module being encoded using by an encryption algorithm performs and a symmetric encryption method which uses an encryption parameter, wherein encryption algorithms and encryption parameters are uniquely respectively assigned to the object modules module;

wherein the memory element of the one object module stores at least two different encryption algorithms and at least two different encryption parameters including the encryption algorithms and the encryption parameters assigned to the object modules, wherein the microprocessor of the one object module selects one of from the stored encryption algorithms and encryption parameters the encryption algorithm and the encryption parameter assigned to an object module to be used with the symmetric encryption method by an identification device for encoding the data communicated by the identification device and [[an]] the object module.

4. (ORIGINAL) The system of claim 3 wherein:

the encryption algorithm to be used by the identification device for encoding the data communicated by the identification device and an object module is assigned by the one object module to the identification device during a single initialization process between the identification device and the one object module.

5. (CURRENTLY AMENDED) An identification device for a keyless authorized access control system having at least two object modules, each object module being assigned to a respective object, wherein the identification device and the object modules have respective bidirectional data communications links between them for communicating encoded

data, the data communicated between the identification device and [[an]] each object module being encoded using by an encryption algorithm that is used to perform and a symmetric encryption method which uses an encryption parameter, wherein encryption algorithms and encryption parameters are uniquely respectively assigned to the object modules module, the identification device comprising:

a microprocessor and a memory element, wherein the memory element stores at least two different encryption algorithms and at least two different encryption parameters including the encryption algorithms and the encryption parameters assigned to the object modules, wherein the microprocessor selects one of from the stored encryption algorithms and encryption parameters the encryption algorithm and the encryption parameter assigned to an object module to be used with the symmetric encryption method for encoding the data to be communicated with [[an]] the object module.

6. (ORIGINAL) The identification device of claim 5 wherein:

the encryption algorithms stored in the memory element are configurable and replaceable through a programming interface.

7. (ORIGINAL) The identification device of claim 5 wherein:

the memory element is integrated in the microprocessor.

8. (CURRENTLY AMENDED) An object module for a keyless authorized access control system having an identification device and at least one other object module, each object module being assigned to a respective object, wherein the identification device and the object modules have respective bidirectional data communications links between them for communicating encoded data, the data communicated between the identification device and an each object module being encoded using by an encryption algorithm that is used to perform and a symmetric encryption method which uses an encryption parameter, wherein encryption algorithms and encryption parameters are uniquely respectively assigned to the object modules module, the object module comprising:

a microprocessor and a memory element, wherein the memory element stores at least two different encryption algorithms and at least two different encryption parameters including the encryption algorithms and the encryption parameters assigned to the object modules, wherein the microprocessor selects one of from the stored encryption algorithms and encryption parameters the encryption algorithm and the encryption parameter assigned to one of the object modules to be used with the symmetric encryption method by the identification device for encoding the data communicated by the identification device and the one of the object modules.

9. (ORIGINAL) The object module of claim 8 wherein:
the encryption algorithms stored in the memory element are configurable and replaceable through a programming interface.